

Inbox Intrusions & Expensive Illusions

When Email Authentication Goes Wrong

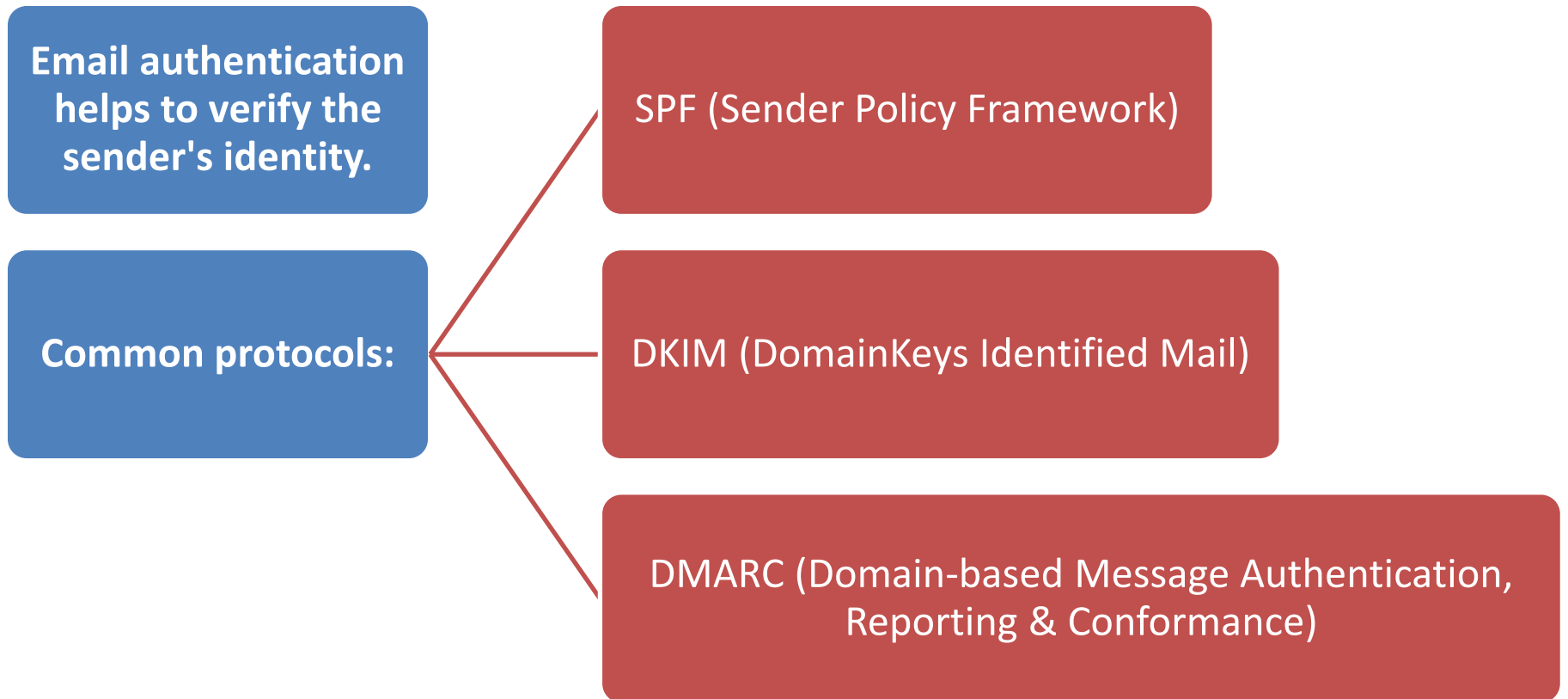
Dana Rubena

ESET Security Day 2025

Agenda

1. Brief Introduction to Email Authentication
2. Case 1: Impersonation & Financial Fraud
3. Case 2: Bypassing Email Protection via Legitimate Service
4. Recommendations
5. Q&A

What Is Email Authentication?



Why Email Authentication Matters



Prevents spoofing and impersonation



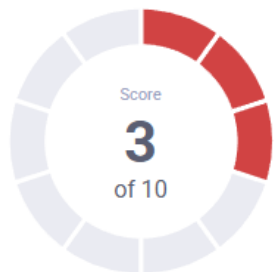
Helps email security systems filter malicious content



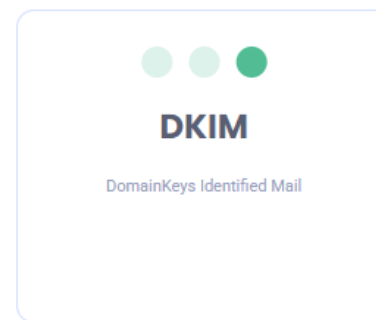
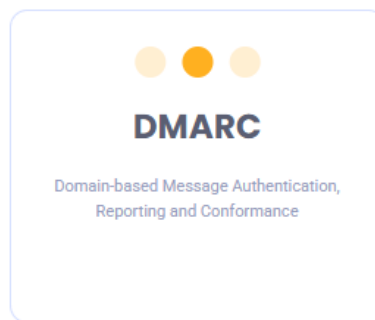
Builds trust in communication

Example of [LegitCorp.de] Domain Security

Overall result ⓘ



DMARC Policy: None



**Authentication
-Results-
Original**

**dkim=pass header.d=LegitCorpde.onmicrosoft.com header.s=selector1-LegitCorpde-onmicrosoft-com;
spf=permerror smtp.mailfrom=sender@LegitCorp.de; dmarc=fail header.from=LegitCorp.de**

Case 1: the Curious Case of the Phantom Bank Change

SCENARIO:

1. **allnexTeam** regularly received invoices from a vendor **Banana Freight** via the email sparklepony@rainbowmail.com.
2. One day, an invoice arrived with updated banking details.
3. Shortly after, a known contact at **Banana Freight** confirmed that the company was *not* changing banks. Another confirmation for the same came via elena.donutss@gmail.com (a known gmail contact for **Banana Freight**), backing this up.
4. Weeks later, **allnexTeam** received another bank change notice from sparklepony@rainbowmail.com, along with official documents. On the same day, similar documents came from elena.donutsss@gmail.com, confirming the bank change.

Email #1

From: Banana Freight <sparklepony@rainbowmail.com>

Sent: Friday, June 27, 2025 2:32 PM

To: allnexTeam@allnex.com

Subject: Re: Bank change

CAUTION: Email from outside allnex. Do not click links or open attachments unless you recognize the sender and know the content is safe.

I hope this message finds you well.

Please find attached the PDF document containing the updated bank account information for your records. Kindly update your system accordingly.

Also, note that the mobile number provided on the letterhead should be used for verbal confirmation of this change.

Please feel free to reach out.

Thank you for your prompt attention.

Best regards,

Elena Donutss

President

Email #2

From: Elena Donutss <elena.donutsss@gmail.com>
Sent: Tuesday, July 15, 2025 10:14 AM
To: allnexTeam@allnex.com
Subject: Re: Phone call

CAUTION: Email from outside allnex. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Please find attached the PDF document containing the updated bank account information for your records. Kindly update your system accordingly.

Also, note that the mobile number provided on the letterhead should be used for verbal confirmation of this change.

Please feel free to reach out.

Thank you for your prompt attention.

Best regards,

Elena Donutss

President

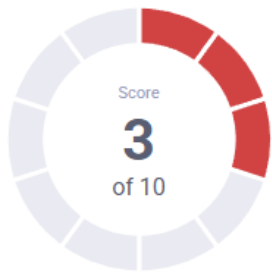
Case 1: the Curious Case of the Phantom Bank Change [cont.]

5. **allnexTeam** ran anti-fraud checks via the contact details provided in the email from elena.donutsss@gmail.com and updated the bank info.
6. The bank account was changed with approval from the supervisor at **allnexTeam**, and invoice was paid.
7. A week later, the real **Banana Freight** called, saying they hadn't received the payment.
8. **allnexTeam** contacted another buyer, **Caramel Iguana**, to validate **Banana Freight** contact info. After calling the correct number, the **Banana Freight** confirmed their email had been hacked and no bank change had ever occurred.

Example of [rainbowmail] Domain Security

Overall result ⓘ

DMARC Policy: Missing



SPF

Sender Policy Framework



DMARC

Domain-based Message Authentication,
Reporting and Conformance



DKIM

DomainKeys Identified Mail

SPF

Valid

Your domain has a valid SPF record. You can track, manage and level up your email authentication standards by using our platform.

Record value: v=spf1 include:_ipspf.yahoo.com ~all

Case 2: Microsoft's Shortcut Through Email Fort Knox

What Is Direct Send?

- Direct Send is a built-in feature in Microsoft Exchange Online (part of Microsoft 365).
- It allows devices like printers or business apps to send emails without needing a password or login.
- It is ON by default for all Microsoft 365 users.

How Hackers Are Exploiting It

- Using Direct Send to bypass email security checks.
- **They send fake emails that look like internal messages (e.g., voicemails or PDFs with QR codes).**
- These emails trick users into clicking malicious links or scanning phishing QR codes.
- Because the emails appear to come from inside the company, they're more likely to be trusted.

Why It Matters

- Many organizations are unaware this feature is active.
- IT teams are struggling to secure it without breaking legitimate services.

Spoofed Email via Direct Send

Öppna nu: Bonus & lönespecifikation 2025 | Sista dag LINXDAG




allnexUser @allnex.com

To allnexUser @allnex.com



Thu 31/07

 This message was sent with High importance.



Allnex_Q3_2025_Volledige_Vergoeding.pdf
21 KB

Direct Send Email Header Artifacts

X-MS-Exchange-CrossTenant-AuthAs	Anonymous
X-MS-Exchange-CrossTenant-AuthSource	DU2PEPF00028D0B.eurprd03.prod.outlook.com
X-MS-Exchange-CrossTenant-FromEntityHeader	Internet
X-MS-Exchange-CrossTenant-Id	969f04f9-877e-415d-9aed-4198a3e758e5
X-MS-Exchange-CrossTenant-Network-Message-Id	a4b4efa4-b7f9-42f5-54d5-08ddd040d848
X-MS-Exchange-CrossTenant-OriginalArrivalTime	31 Jul 2025 14:45:08.0363 (UTC)
X-MS-Exchange-Organization-AuthAs	Anonymous
X-MS-Exchange-Organization-AuthSource	DU2PEPF00028D0B.eurprd03.prod.outlook.com
X-MS-Exchange-Organization-ExpirationInterval	1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationStartTime	31 Jul 2025 14:45:08.1581 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason	OriginalSubmit
X-MS-Exchange-Organization-MessageDirectionality	Incoming
X-MS-Exchange-Organization-Network-Message-Id	a4b4efa4-b7f9-42f5-54d5-08ddd040d848
X-MS-Exchange-Organization-SCL	-1

Direct Send Email Header Artifacts [cont.]

From	allnexUser @allnex.com>
Authentication-Results	spf=fail (sender IP is 51.89.87.86) smtp.mailfrom=allnex.com; dkim=none (message not signed) header.d=none; dmarc=fail action=oreject header.from=allnex.com; compauth=none reason=451
Content-Disposition	attachment
Content-Transfer-Encoding	base64
Content-Type	application/pdf
Date	Thu, 31 Jul 2025 14:45:07 +0000
Importance	High
Message-ID	<2af8daff-d82e-3a10-dd91-6ab3d1ce41d3@allnex.com>
MIME-Version	1.0
Received	from [127.0.0.1] (51.89.87.86) by DU2PEPF00028D0B.mail.protection.outlook.com (10.167.242.171) with Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15
Received-SPF	Fail (protection.outlook.com: domain of allnex.com does not designate 51.89.87.86 as permitted sender) receiver=protection.outlook.com; client-ip=51.89.87.86; helo=[127.0.0.1];
Reply-To	<andrei.ciubotaru@wipindustries-eu.com>
Return-Path	allnexUser @allnex.com
Subject	Öppna nu: Bonus & lönespecifikation 2025 Sista dag LINXDAG
To	allnexUser @allnex.com>

Recommendations

- Enforce SPF, DKIM, and DMARC
- Use DMARC with a **reject** policy
- Implement email header analysis tools
- Configure Microsoft Exchange Online to **Reject Direct Send** emails, unless sent via specified connectors
- Conduct phishing tests and Business Email Compromise (BEC) simulations to educate users
- Learn to understand headers to spot malicious emails



Q&A

What surprised you the most about these cases?
(Open floor for questions)

